What is claimed is

1. Method for modular multiplying a multiplicand by a multiplier using a modulus, said multiplicand, said multiplier and said modulus being polynomials of a variable, with a cryptographic calculation, said multiplicand, said multiplier and said modulus being parameters in said cryptographic calculation, said method comprising the following steps:

(a) performing a multiplication look-ahead method to obtain a multiplication shift value, said multiplication shift value being incremented at a power of said multiplier, which is not present in the multiplier polynomial;

(b) multiplying said variable raised to the power of said multiplication shift value by an intermediate result polynomial to obtain a shifted intermediate result polynomial;

(c) performing a reduction look-ahead method to obtain a reduction shift value, said reduction shift value being equal to the difference of the degree of said shifted intermediate result polynomial and the degree of said modulus polynomial;

(d) multiplying said variable raised to the power of said reduction shift value by said modulus polynomial to obtain a shifted modulus polynomial;

(e) summing said shifted intermediate result polynomial and said multiplicand and subtracting said shifted modulus

polynomial to obtain an updated intermediate result polynomial; and

(f) repeating steps (a) to (e) until all the powers of said multiplier have been processed, wherein in the repetition of steps (a) to (e)

in step (d) said updated intermediate result polynomialof the previous step (e) is used as said intermediate result polynomial, and

in step (c) said shifted polynomial of the previous step (d) is used as a modulus polynomial.

2. Method according to claim 1, wherein said multiplying in step (d) is carried out by shifting said intermediate result polynomial by a number of digits equalling said multiplication shift value, and

wherein said multiplying in step (d) is carried out by shifting said modulus polynomial by a number of digits equalling said reduction shift value.

3. Method according to claim 1, wherein coefficients of said polynomials can only take the values "0" or "1", and

wherein said summing and subtracting in step (e) is carried out by bitwise XORing said intermediate result polynomial, said multiplicand and said shifted modulus polynomial.

4. Method according to claim 1, wherein said step of said reduction look-ahead method to obtain a reduction shift value comprises the following steps:

determining an auxiliary shift value so that the degree of said modulus polynomial and the degree of said updated intermediate result polynomial of the previous step (e) multiplied by a variable which is raised to the power of said auxiliary shift value are equal, and

forming the difference of said multiplication shift value and said auxiliary shift value to obtain said reduction shift value.

5. Method according to claim 4, wherein said step of performing said multiplication look-ahead method and said step of determining said auxiliary shift value are carried out parallel to each other.

6. Method according to claim 1,

wherein said multiplication shift value is limited to a maximum multiplication shift value,

wherein said step of performing said multiplication shift method comprises the following steps:

if said multiplication shift value equals said maximum multiplication shift value,

equating said multiplication shift value with said maximum shift value,

creating a multiplication look-ahead parameter with a predetermined value, and

wherein said step of summing comprises the following steps:

if said multiplication look-ahead parameter has said predetermined value,

summing only said predetermined intermediate result polynomial and said shifted modulus polynomial.

7. Apparatus for modular multiplying a multiplicand by a multiplier using a modulus, said multiplicand, said multiplier and said modulus being polynomials of a variable, within a cryptographic calculation, said multiplicand, said multiplier and said modulus being parameters in said cryptographic calculation, said apparatus comprising:

(a) means for performing a multiplication look-ahead method to obtain a multiplication shift value, said multiplication shift value being incremented at a power of said multiplier, which is not present in the multiplier polynomial;

(b) means for multiplying said variable which is raised to the power of said multiplication shift value by an intermediate result polynomial to obtain a shifted intermediate result polynomial;

(c) means for performing a reduction look-ahead method to obtain a reduction shift value, said reduction shift value being equal to the difference of the degree of said shifted intermediate result polynomial and the degree of said modulus polynomial;

(d) means for multiplying said variable which is raised to the power of said reduction shift value by said modulus polynomial to obtain a shifted modulus polynomial;

(e) means for summing said shifted intermediate result polynomial and said multiplicand and subtracting said shifted modulus polynomial to obtain an updated intermediate result polynomial; and

(f) means for repeatedly controlling said means (a) to (e) until all the powers of said multiplier have been processed, wherein in a repeated control of said means (a) to (e)

said means for multiplying to obtain a shifted intermediate result polynomial is arranged to use said updated intermediate result polynomial of the previous control of said means for summing as an intermediate result polynomial, and

said means for performing a reduction look-ahead method is arranged to use, in a repeated control, as the modulus polynomial, said shifted modulus polynomial of the previous control of said means for multiplying to obtain a shifted modulus polynomial.

8. Apparatus according to claim 7, wherein said means for multiplying to obtain a shifted intermediate result polynomial and said means for multiplying to obtain a shifted modulus polynomial are implemented as controllable shift registers to perform, depending on said multiplication shift value or on said reduction shift value, a shift of the register contents by a corresponding number of digits.

9. Apparatus according to claim 7, wherein said means for summing and for subtracting is carried out as bitwise XORing said intermediate result polynomial, said multiplicand and said shifted modulus polynomial.

10. Apparatus according to claim 7, said means for summing and subtracting comprising:

a counter with three input lines and two output lines, wherein a bit of said intermediate result polynomial can be applied to a first input line, wherein a bit of said multiplicand can be applied to a second input line, and wherein a bit of said shifted modulus polynomial can be applied to a third input line;

a full adder with three inputs and one output, a low-order output of said counter being connected to a higher order input line of said full adder;

a switch connected between a higher order output line of said counter and a middle input of a full adder for a higher order bit; and

a control unit for opening said switch when polynomials are to be processed.

11. Apparatus according to claim 7, formed as calculating unit for multiplying the multiplicand by the multiplier using the modulus

the calculating unit further optionally being formed for multiplying a multiplicand integer by a multiplier integer using a modulus integer,

means for summing being formed as three-operands adder comprising a carry disabling means for combining either the integer operands or one polynomial intermediate result, said shifted modulus and said multiplicand

means further comprising a control means for controlling said carry disabling means so that a carry is deactivated when polynomial operands are processed and so that the carry is activated when integer operands are processed.

12. Apparatus according to claim 11, said three-operands adder with a carry disabling means comprising:

a counter with three input lines and two output lines, wherein a bit of said intermediate result can be applied to a first input line, wherein a bit of said multiplicand can be applied to a second input line, and wherein a bit of said shifted modulus can be applied to a third input line;

a full adder with three inputs and one output, a low-order output of said counter being connected to a higher order input line of said full adder;

a switch being connected between a higher order output line of said counter and a middle input of a full adder for a next higher bit; and

a control unit for opening said switch when polynomials are to be processed.

13. Apparatus according to claim 12, wherein a plurality of three-operands adders are present, the number of three-

operands adders present being greater than or equal to the number of digits of the modulus integer or the modulus.